

EXHIBIT 7

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRIAN KEMP, ET AL.,
Defendants.**

**DECLARATION OF DUNCAN
BUELL IN SUPPORT OF
MOTION FOR PRELIMINARY
INJUNCTION**

Civil Action No. 1:17-CV-2989-AT

Pursuant to 28 U.S. § 1746, I, Duncan A. Buell, declare under penalty of perjury that the following is true and correct:

1. I am a professor of Computer Science and Engineering at the University of South Carolina. I have been asked by counsel for Donna Curling, Donna Price, and Jeffrey Schoenberg to offer observations regarding the security of the DRE systems and their use in Georgia elections, based on my years of experience in the field of election security. I previously submitted an Affidavit on behalf of the Plaintiffs in this matter (Dkt. No. 15-2 Ex. G), a copy of which has been attached hereto as **Exhibit A**.

2. In 1971, I earned a B.S. in Mathematics from the University of Arizona. The following year, I earned an M.A. in Mathematics from the University

been successful. As a result, there are serious, well-known risks associated with the use of the Diebold DREs used in Georgia.

8. One of the primary risks of the system is manipulation through the insertion of malware. Given the manner in which Georgia operates its elections through a central server, one need only access this central server in order to inject malicious code that could cause “disruption” (errors or failures) or “corruption” (the altering, addition, or deletion of votes) to a significant number of machines.

9. It is important to keep in mind that any malware injected does not have to be immediately executable, but can be written so as to execute only under certain conditions, perhaps only on Election Day, or otherwise tailored to meet the goals of the person attacking the system. Unfortunately, there is a wide array of coding techniques that could be employed to launch a targeted attack on a particular election, such as implementing a code to alter every one out of every 20 votes. In my experience, any sophisticated attack will likely involve multiple layers of code that are not only undetectable during an attack, but are “self-deleting” after they have been fully executed.

10. The risks of the DRE system software are exacerbated by the fact that there is no ability to audit results of any given election. As a result, in those instances in which there is a breach in protocol (whether intentional through one of

become available. At the time Mr. Logan accessed the central server in October 2016, the Drupal SQL vulnerability had been reported nearly two years earlier. In my nine years as chair of the Department of Computer Science and Engineering at the University of South Carolina, with a year in that period when I served as Interim Dean of the college, I was the supervisor for the college's network systems administrator. I can attest that monitoring news lists for vulnerabilities was a routine and ongoing activity and that patches and updates were made as soon as they became available and reliable, even at the occasional cost of lost productivity due to small amounts of downtime.

15. The prudent and professional systems administrators, when alerted to the potential of an unknown vulnerability, will know that it is critical to respond quickly in order to validate the risk and take whatever steps necessary to correct the vulnerability. Based on my review of material provided to date, these steps were not taken until March 2017 at the earliest, and to date, I have not seen evidence indicating that the proper corrective steps have been taken.

Columbia, South Carolina
Dated: August 7, 2018



DUNCAN A. BUELL